

On the Diophantine equation $pq = x^2 + ny^2$

JA KYUNG KOO AND DONG HWA SHIN*

Abstract

Let n be a positive integer. We investigate pairs of distinct odd primes p and q not dividing n for which the Diophantine equations $pq = x^2 + ny^2$ have integer solutions in x and y . As its examples we classify all such pairs of p and q when $n = 5$ and 14 .

1 Introduction

In a letter to Blaise Pascal dated September 25 in 1654 Fermat announced that for primes p and q

$$(1) \quad p, q \equiv 3, 7 \pmod{20} \implies pq = x^2 + 5y^2 \text{ for some } x, y \in \mathbb{Z}.$$

And, Lagrange [6] first noted that

$$p \equiv 3, 7 \pmod{20} \implies p = 2x^2 + 2xy + 3y^2 \text{ for some } x, y \in \mathbb{Z}.$$

He then presented the identity

$$(2) \quad (2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2,$$

which completes the proof.

On the other hand, what can we say about the other direction of (1)? As far as we understand, not much has been known in this theme so far. More generally, let n be a positive integer, and let p and q be distinct odd primes not dividing n . In this paper

2010 *Mathematics Subject Classification*. Primary 11E25; Secondary 11E16.

Key words and phrases. Binary quadratic forms, representations.

The first named author was partially supported by the NRF of Korea grant funded by MISP (2013042157). *The corresponding author was supported by Hankuk University of Foreign Studies Research Fund of 2014.

we shall find an equivalent condition under which the product pq can be represented by the principal form $x^2 + ny^2$ (Theorem 4.1). To this end, we shall review some classical facts about form class groups and ideal class groups (§2–3), from which we are able to give a satisfactory answer to the question above and to the solvability of the Diophantine equation $pq = x^2 + 14y^2$ (Examples 5.1 and 5.2) as well.

2 Binary quadratic forms

We first introduce a general version of the identity (2).

LEMMA 2.1. *Let $a, b, c \in \mathbb{Z}$ with $n = -b^2 + ac$. We have the identity*

$$(ax^2 + 2bxy + cy^2)(az^2 + 2bzw + cw^2) = (axz + bxw + byz + cyw)^2 + n(xw - yz)^2.$$

PROOF. Immediate. □

Let $f(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form (for short, a form). It is said to be *primitive* if its coefficients a , b and c are relatively prime. Let m be an integer. We say that m is *represented* by $f(x, y)$ if the equation $m = f(x, y)$ has an integer solution in x and y . Moreover, if such x and y are relatively prime, then we say that m is *properly represented* by $f(x, y)$.

Let $f(x, y)$ and $g(x, y)$ be primitive positive definite forms of the same discriminant. We say that they are *equivalent* (respectively, *properly equivalent*) if there is an element $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ of $\text{GL}_2(\mathbb{Z})$ (respectively, $\text{SL}_2(\mathbb{Z})$) such that

$$f(x, y) = g(px + qy, rx + sy).$$

The equivalence and properly equivalence of forms are indeed equivalence relations. Furthermore, two equivalent forms represent the same numbers [1, pp.24–25].

For a negative integer D such that $D \equiv 0, 1 \pmod{4}$ we let $C(D)$ be the set of all properly equivalence classes of primitive positive definite forms of discriminant D . As is well-known the Dirichlet composition makes $C(D)$ into a finite abelian group, called the *form class group* of discriminant D [1, Theorem 3.9]. We denote by $h(D)$ the order of the group $C(D)$.

We call a primitive positive definite form $ax^2 + bxy + cy^2$ a *reduced form* if the coefficients a , b and c satisfy

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } |b| = 0 \text{ or } a = c.$$

Then, every primitive positive definite form of discriminant D is properly equivalent to a unique reduced form of the same discriminant [1, Theorem 2.8]. Hence $h(D)$ is equal to the number of reduced forms of discriminant D .

PROPOSITION 2.2. *Let n be a positive integer and p be an odd prime not dividing n . Then we get the assertion*

$$\left(\frac{-n}{p}\right) = 1 \iff p \text{ is represented by a reduced form of discriminant } -4n.$$

PROOF. See [1, Corollary 2.6]. □

Let n be a positive integer. Euler called n a *convenient number* if it satisfies the following properties:

Let m be an odd positive integer relatively prime to n which is properly represented by $x^2 + ny^2$. If the equation $m = x^2 + ny^2$ has only one solution with $x, y \geq 0$, then m is a prime.

We say that two primitive positive definite forms of discriminant D (< 0) are in the same *genus* if they represent the same values in $(\mathbb{Z}/D\mathbb{Z})^\times$. Then it is well-known that n is a convenient number if and only if every genus of discriminant $-4n$ consists of a single properly equivalence class [1, Proposition 3.24] (see also [4], [9] and [10]).

3 Ideal class groups

Let K be an imaginary quadratic field of discriminant d_K and \mathcal{O}_K be its ring of integers. Let \mathcal{O} be the order conductor f (> 0) in K , so its discriminant D satisfies the relation $D = f^2 d_K$. We denote by $I(\mathcal{O})$ the group of all proper fractional \mathcal{O} -ideals (under multiplication), and by $P(\mathcal{O})$ its subgroup of all principal \mathcal{O} -ideals. We call the associated quotient group $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ the *ideal class group* of the order \mathcal{O} . Then we will relate this ideal class group $C(\mathcal{O})$ with the form class group $C(D)$ defined in §2 via the following isomorphism

$$(3) \quad \begin{array}{ccc} C(D) & \xrightarrow{\sim} & C(\mathcal{O}) \\ \text{class of } ax^2 + bxy + cy^2 & \mapsto & \text{class of } [a, (-b + \sqrt{D})/2] \end{array}$$

[1, Theorem 7.7(ii)].

LEMMA 3.1. *Let $f(x, y)$ be a reduced form of discriminant D and m be a positive integer. Then,*

$$m \text{ is represented by } f(x, y) \iff m = N_{\mathcal{O}}(\mathfrak{a}) \ (= |\mathcal{O}/\mathfrak{a}|) \text{ for some } \mathcal{O}\text{-ideal } \mathfrak{a} \\ \text{in the corresponding ideal class in } C(\mathcal{O}).$$

PROOF. See [1, Theorem 7.7(iii)]. □

Furthermore, let $I(\mathcal{O}, f)$ be the subgroup of $I(\mathcal{O})$ consisting of all proper fractional \mathcal{O} -ideals prime to f , and let $I_K(f)$ be the group of all fractional ideals of K prime to f . Then we have an isomorphism

$$(4) \quad \begin{array}{ccc} \phi_f : I_K(f) & \xrightarrow{\sim} & I(\mathcal{O}, f) \\ \mathfrak{a} & \mapsto & \mathfrak{a} \cap \mathcal{O} \end{array}$$

which preserves norms, namely $N_{\mathcal{O}_K}(\mathfrak{a}) = N_{\mathcal{O}}(\mathfrak{a} \cap \mathcal{O})$. Its inverse map ϕ_f^{-1} is given by

$$\phi_f^{-1}(\mathfrak{b}) = \mathfrak{b}\mathcal{O}_K \quad (\mathfrak{b} \in I(\mathcal{O}, f))$$

[1, Proposition 7.20].

On the other hand, we know by the existence theorem of class field theory that there exists a unique abelian extension $H_{\mathcal{O}}$ of K whose Galois group satisfies

$$\text{Gal}(H_{\mathcal{O}}/K) \simeq C(\mathcal{O})$$

([3, Chapters IV and V] and [1, Proposition 7.22]). We call this extension $H_{\mathcal{O}}$ the *ring class field* of the order \mathcal{O} .

PROPOSITION 3.2. *Let n be a positive integer and $H_{\mathcal{O}}$ be the ring class field of the order $\mathcal{O} = [1, \sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$. Let $f_n(x)$ be the minimal polynomial of a real algebraic integer which generates $H_{\mathcal{O}}$ over K . If an odd prime p divides neither n nor the discriminant of $f_n(x)$, then*

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \iff \left(\frac{-n}{p}\right) = 1 \text{ and } f_n(x) \equiv 0 \pmod{p} \\ \text{has an integer solution.}$$

PROOF. See [1, Theorem 9.2]. □

REMARK 3.3. By the main theorem of complex multiplication, the singular value $j(\mathcal{O})$ of the elliptic modular function j generates $H_{\mathcal{O}}$ over K as a real algebraic integer [7, Chapter 5, Theorem 4 and Chapter 10, Theorem 5]. However, its minimal polynomial has too large integer coefficients for practical use (such as Proposition 3.2). On the other hand, one can refer to [2], [5] and [8] for other smaller generators of $H_{\mathcal{O}}$ in terms of the singular values of Weber functions and eta-quotients.

4 Products of two primes in the form $x^2 + ny^2$

We are ready to prove our main theorem concerning the Diophantine equation $pq = x^2 + ny^2$.

THEOREM 4.1. *Let n be a positive integer, and let p and q be distinct odd primes not dividing n . Then,*

$$pq = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \iff \text{there is a reduced form of discriminant } -4n \text{ representing both } p \text{ and } q.$$

PROOF. First, assume that there exists a reduced form $f(x, y) = ax^2 + bx + c$ of discriminant $-4n$ representing both p and q . Then we have

$$p = f(x_1, y_1) \text{ and } q = f(x_2, y_2) \text{ for some } x_1, y_1, x_2, y_2 \in \mathbb{Z}.$$

It follows from $b^2 - 4ac = -4n$ that b is an even integer. So we achieve by Lemma 2.1

$$pq = f(x_1, y_1)f(x_2, y_2) = (ax_1x_2 + (b/2)x_1y_2 + (b/2)y_1x_2 + cy_1y_2)^2 + n(x_1y_2 - y_1x_2)^2.$$

This yields that pq can be written in the form $x^2 + ny^2$ for some $x, y \in \mathbb{Z}$.

Conversely, assume that

$$(5) \quad pq = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z}.$$

Since p and q are distinct odd primes not dividing n by hypothesis, we deduce from (5)

$$\left(\frac{-n}{p}\right) = \left(\frac{-n}{q}\right) = 1.$$

This implies that both p and q split in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$. Let

$$(6) \quad p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} \text{ and } q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$$

be the prime ideal factorizations of $p\mathcal{O}_K$ and $q\mathcal{O}_K$, respectively. We then derive that

$$\begin{aligned} (pq)\mathcal{O}_K &= (x^2 + ny^2)\mathcal{O}_K \quad \text{by (5)} \\ &= (x + \sqrt{-n}y)\mathcal{O}_K \overline{(x + \sqrt{-n}y)\mathcal{O}_K} \\ &= (p\mathcal{O}_K)(q\mathcal{O}_K) \\ &= (\mathfrak{p}\bar{\mathfrak{p}})(\mathfrak{q}\bar{\mathfrak{q}}) \quad \text{by (6)} \\ &= (\mathfrak{p}\mathfrak{q})\overline{(\mathfrak{p}\mathfrak{q})} \quad (= (\mathfrak{p}\bar{\mathfrak{q}})\overline{(\mathfrak{p}\bar{\mathfrak{q}})}). \end{aligned}$$

Thus without loss of generality we may assume by the uniqueness of prime ideal factorization in \mathcal{O}_K that

$$(7) \quad \mathfrak{p}\mathfrak{q} = (x + \sqrt{-n}y)\mathcal{O}_K.$$

On the other hand, let $\mathcal{O} = [1, \sqrt{-n}]$, which is the order in K of discriminant $D = f^2d_K = -4n$. Here, d_K is the discriminant of K and f is the conductor of \mathcal{O} . Let $f(x, y)$

be the reduced form of discriminant D corresponding to the ideal class $C = [\bar{\mathfrak{p}} \cap \mathcal{O}]$ in $C(\mathcal{O})$ via the isomorphism in (3). Then the norm $N_{\mathcal{O}}(\bar{\mathfrak{p}} \cap \mathcal{O}) = N_{\mathcal{O}_K}(\bar{\mathfrak{p}}) = p$ can be represented by $f(x, y)$ by Lemma 3.1. Furthermore, we attain that in $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$,

$$\begin{aligned}
[\mathfrak{q} \cap \mathcal{O}] &= [p\mathcal{O}][\mathfrak{q} \cap \mathcal{O}] \quad \text{since } p\mathcal{O} \in P(\mathcal{O}) \\
&= [p\mathcal{O}_K \cap \mathcal{O}][\mathfrak{q} \cap \mathcal{O}] \\
&\quad \text{by considering the isomorphism } \phi_f \text{ in (4) and its inverse map } \phi_f^{-1} \\
&= [(p\mathcal{O}_K)\mathfrak{q} \cap \mathcal{O}] \quad \text{by the homomorphism property of } \phi_f \\
&= [\mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q} \cap \mathcal{O}] \quad \text{by (6)} \\
&= [\mathfrak{p}\mathfrak{q} \cap \mathcal{O}][\bar{\mathfrak{p}} \cap \mathcal{O}] \quad \text{again by the homomorphism property of } \phi_f \\
&= [(x + \sqrt{-ny})\mathcal{O}_K \cap \mathcal{O}][\bar{\mathfrak{p}} \cap \mathcal{O}] \quad \text{by (7)} \\
&= [(x + \sqrt{-ny})\mathcal{O}][\bar{\mathfrak{p}} \cap \mathcal{O}] \quad \text{because } x + \sqrt{-ny} \in \mathcal{O} \\
&= [\bar{\mathfrak{p}} \cap \mathcal{O}] \quad \text{since } (x + \sqrt{-ny})\mathcal{O} \in P(\mathcal{O}) \\
&= C.
\end{aligned}$$

Therefore the norm $N_{\mathcal{O}}(\mathfrak{q} \cap \mathcal{O}) = N_{\mathcal{O}_K}(\mathfrak{q}) = q$ is also represented by $f(x, y)$ by Lemma 3.1. This completes the proof of the theorem. \square

5 Examples

In this section we shall present a couple of concrete examples of Theorem 4.1.

EXAMPLE 5.1. First we consider the question raised in §1 about the Diophantine equation $pq = x^2 + 5y^2$. Let $n = 5$. There are two reduced forms of discriminant $-4n = -20$, namely

$$x^2 + 5y^2 \text{ and } 2x^2 + 2xy + 3y^2.$$

One can then readily check that

$$\begin{cases} x^2 + 5y^2 & \text{represents } 1, 9 \text{ in } (\mathbb{Z}/20\mathbb{Z})^\times, \\ 2x^2 + 2xy + 3y^2 & \text{represents } 3, 7 \text{ in } (\mathbb{Z}/20\mathbb{Z})^\times \end{cases}$$

[1, (2.20)]. This shows that there are two genera of discriminant -20 each consisting of a single class, and hence $n = 5$ is a convenient number.

On the other hand, we obtain by Proposition 2.2 that for an odd prime p other than 5

$$\begin{aligned}
p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2 \text{ for some } x, y \in \mathbb{Z} &\iff \left(\frac{-5}{p}\right) = 1 \\
&\iff p \equiv 1, 3, 7, 9 \pmod{20}.
\end{aligned}$$

Therefore we conclude by Theorem 4.1 that for distinct odd primes p and q other than 5

$$pq = x^2 + 5y^2 \text{ for some } x, y \in \mathbb{Z} \iff \begin{cases} x^2 + 5y^2, \text{ or} \\ 2x^2 + 2xy + 3y^2 \end{cases} \text{ both } p \text{ and } q \text{ are represented by}$$

$$\iff \begin{cases} p, q \equiv 1, 9 \pmod{20}, \text{ or} \\ p, q \equiv 3, 7 \pmod{20}. \end{cases}$$

EXAMPLE 5.2. Let $n = 14$. We then have four reduced forms of discriminant $-4n = -56$

$$x^2 + 14y^2, \quad 2x^2 + 7y^2 \text{ and } 3x^2 \pm 2xy + 5y^2,$$

and we see that

$$(8) \quad \begin{cases} x^2 + 14y^2, \quad 2x^2 + 7y^2 & \text{represents } 1, 9, 15, 23, 25, 39 \text{ in } (\mathbb{Z}/56\mathbb{Z})^\times, \\ 3x^2 \pm 2xy + 5y^2 & \text{represents } 3, 5, 13, 19, 27, 45 \text{ in } (\mathbb{Z}/56\mathbb{Z})^\times \end{cases}$$

[1, (2.21)]. This shows that $n = 14$ is a non-convenient number. Observe that $3x^2 + 2xy + 5y^2$ and $3x^2 - 2xy + 5y^2$ are equivalent, but $x^2 + 5y^2$ and $2x^2 + 7y^2$ are not. Furthermore, we obtain by Proposition 2.2 that for an odd prime p not dividing 14

$$\begin{aligned} & p \text{ is represented by one of the above reduced forms} \\ \iff & \left(\frac{-14}{p} \right) = 1 \\ \iff & p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}. \end{aligned}$$

Let $K = \mathbb{Q}(\sqrt{-14})$ and $\mathcal{O} = \mathcal{O}_K = [1, \sqrt{-14}]$. Then we know that $H_{\mathcal{O}}$ is generated by a real algebraic integer $\alpha = \sqrt{2\sqrt{2} - 1}$ whose minimal polynomial over K is $(x^2 + 1)^2 - 8$ with discriminant $-2^{14} \cdot 7$ [1, Proposition 5.31]. Thus we deduce by Proposition 3.2 that for an odd prime p not dividing 14

$$(9) \quad p = x^2 + 14y^2 \text{ for some } x, y \in \mathbb{Z} \iff \left(\frac{-14}{p} \right) = 1 \text{ and } p \in S,$$

where

$$S = \{\text{primes } p \mid (x^2 + 1)^2 \equiv 8 \pmod{p} \text{ has an integer solution}\}$$

[1, Theorem 5.33].

Suppose that there exists an odd prime p not dividing 14 which is represented by $x^2 + 14y^2$ and $2x^2 + 7y^2$, simultaneously. Let

$$(10) \quad p = x_1^2 + 14y_1^2 \quad \text{for some } x_1, y_1 \in \mathbb{Z},$$

$$(11) \quad p = 2x_2^2 + 7y_2^2 \quad \text{for some } x_2, y_2 \in \mathbb{Z}.$$

Here, x_1, y_1, x_2, y_2 are all nonzero integers modulo p because p is relatively prime to 14. We claim by (10) that p splits in $K = \mathbb{Q}(\sqrt{-14})$ and

$$(12) \quad p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} \quad \text{with } \mathfrak{p} = (x_1 + \sqrt{-14}y_1)\mathcal{O}_K \text{ and } \bar{\mathfrak{p}} = (x_1 - \sqrt{-14}y_1)\mathcal{O}_K.$$

Moreover, since 2 is ramified in K , we have

$$(13) \quad 2\mathcal{O}_K = \mathfrak{a}\bar{\mathfrak{a}} \text{ with } \mathfrak{a} = \bar{\mathfrak{a}}.$$

We then see that

$$\begin{aligned} (2p)\mathcal{O}_K &= (4x_2^2 + 14y_2^2)\mathcal{O}_K \quad \text{by (11)} \\ &= (2x_2 + \sqrt{-14}y_2)\mathcal{O}_K \overline{(2x_2 + \sqrt{-14}y_2)\mathcal{O}_K} \\ &= (2\mathcal{O}_K)(p\mathcal{O}_K) \\ &= (\mathfrak{a}\bar{\mathfrak{a}})(\mathfrak{p}\bar{\mathfrak{p}}) \quad \text{by (12) and (13)} \\ &= (\mathfrak{a}\mathfrak{p})\overline{(\mathfrak{a}\mathfrak{p})} \quad (= (\mathfrak{a}\bar{\mathfrak{p}})\overline{(\mathfrak{a}\bar{\mathfrak{p}})}). \end{aligned}$$

So, without loss of generality we may assume that $\mathfrak{a}\mathfrak{p} = (2x_2 + \sqrt{-14}y_2)\mathcal{O}_K$. And, since \mathfrak{p} is principal by (12), we get that \mathfrak{a} is also principal, say, $\mathfrak{a} = (u + \sqrt{-14}v)\mathcal{O}_K$ for some $u, v \in \mathbb{Z}$. It then follows that

$$2 = N_{\mathcal{O}_K}(\mathfrak{a}) = N_{K/\mathbb{Q}}(u + \sqrt{-14}v) = u^2 + 14v^2.$$

But there is no such pair of integers u and v , which yields a contradiction. Hence we conclude that

$$(14) \quad \begin{array}{l} \text{there is no odd prime } p \text{ not dividing 14} \\ \text{which can be represented by both } x^2 + 14y^2 \text{ and } 2x^2 + 7y^2. \end{array}$$

Therefore we achieve by Theorem 4.1, Proposition 2.2, (8), (9) and (14) that for distinct odd primes p and q not dividing 14

$$\begin{aligned} & pq = x^2 + 14y^2 \text{ for some } x, y \in \mathbb{Z} \\ \iff & \text{ both } p \text{ and } q \text{ are represented by } \begin{cases} x^2 + 14y^2, \text{ or} \\ 2x^2 + 7y^2, \text{ or} \\ 3x^2 + 2xy + 5y^2 \end{cases} \\ \iff & \begin{cases} p, q \equiv 1, 9, 15, 23, 25, 39 \pmod{56} \text{ and } p, q \in S, \text{ or} \\ p, q \equiv 1, 9, 15, 23, 25, 39 \pmod{56} \text{ and } p, q \notin S, \text{ or} \\ p, q \equiv 3, 5, 13, 19, 27, 45 \pmod{56}. \end{cases} \end{aligned}$$

References

- [1] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989.
- [2] A. Gee, *Class invariants by Shimura's reciprocity law*, J. Théor. Nombres Bordeaux 11 (1999), no. 1, 45–72.
- [3] G. J. Janusz, *Algebraic Number Fields*, 2nd edition, Grad. Studies in Math. 7, Amer. Math. Soc., Providence, R. I., 1996.
- [4] E. Kani, *Idoneal numbers and some generalizations*, Ann. Sci. Math. Québec 35 (2011), no. 2, 197–227.
- [5] J. K. Koo, D. H. Shin and D. S. Yoon, *Ring class fields by smaller generators*, <http://arxiv.org/abs/1404.3282>.
- [6] J. L. Lagrange, *Oeuvres*, Vol. 3, Gauthier-Villars, Paris, 1869.
- [7] S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd edition, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.
- [8] R. Schertz, *Complex multiplication*, New Math. Monographs 15, Cambridge University Press, Cambridge, 2010.
- [9] A. Weil, *Number Theory: An Approach Through History; From Hammurapi to Legendre*, Birkhäuser Boston, Inc., Boston, MA, 1984.
- [10] P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. 22 (1973), 117–124.

DEPARTMENT OF MATHEMATICAL SCIENCES
KAIST
DAEJEON 305-701
REPUBLIC OF KOREA

E-mail address: jkkoo@math.kaist.ac.kr

DEPARTMENT OF MATHEMATICS
HANKUK UNIVERSITY OF FOREIGN STUDIES
YONGIN-SI, GYEONGGI-DO 449-791
REPUBLIC OF KOREA

E-mail address: dhshin@hufs.ac.kr